Palo Alto Networks informó que actores de amenazas podrían haber intentado explotar sin éxito una vulnerabilidad crítica de seguridad recientemente divulgada desde el 9 de abril de 2026.

La vulnerabilidad identificada como CVE-2026-0300 (puntaje CVSS: 9.3/8.7) corresponde a un desbordamiento de búfer en el servicio User-ID Authentication Portal del software PAN-OS de Palo Alto Networks. Este fallo podría permitir que un atacante no autenticado ejecute código arbitrario con privilegios de root mediante el envío de paquetes especialmente manipulados.

😖Aunque las correcciones comenzarán a distribuirse a partir del 13 de mayo de 2026, la compañía recomendó a los clientes proteger el acceso al portal User-ID Authentication Portal de PAN-OS restringiéndolo únicamente a zonas confiables o deshabilitándolo completamente si no está en uso.☹

En un aviso publicado el miércoles, la empresa de ciberseguridad indicó que tiene conocimiento de una explotación limitada de la falla. La actividad está siendo rastreada bajo el nombre CL-STA-1132, un presunto grupo de amenazas patrocinado por un Estado cuya procedencia aún no ha sido determinada.☹

"El atacante detrás de esta actividad explotó CVE-2026-0300 para lograr ejecución remota de código (RCE) sin autenticación en el software PAN-OS. Tras una explotación exitosa, el atacante logró inyectar shellcode dentro de un proceso worker de nginx", señaló Unit 42 de Palo Alto Networks.

La firma de ciberseguridad explicó que detectó intentos fallidos de explotación contra un dispositivo PAN-OS desde el 9 de abril de 2026. Aproximadamente una semana después, los atacantes consiguieron ejecutar código de manera remota en el dispositivo e inyectar shellcode exitosamente.

Una vez obtenido el acceso inicial, los actores maliciosos procedieron a eliminar mensajes del kernel relacionados con fallos, borrar registros de errores de nginx y eliminar archivos core dump con el objetivo de ocultar sus actividades.

Las acciones posteriores a la intrusión incluyeron tareas de reconocimiento sobre Active Directory (AD) y el despliegue de cargas adicionales como EarthWorm y ReverseSocks5 en un segundo dispositivo el 29 de abril de 2026. Ambas herramientas han sido utilizadas anteriormente por distintos grupos de hackers vinculados con China.

"Durante los últimos cinco años, actores estatales involucrados en ciberespionaje han centrado cada vez más sus esfuerzos en activos tecnológicos de borde de red, incluyendo firewalls, routers, dispositivos IoT, hipervisores y diversas soluciones VPN, los cuales ofrecen accesos privilegiados y, con frecuencia, carecen de registros robustos y agentes de seguridad presentes en endpoints tradicionales", indicó Unit 42.

"La dependencia de los atacantes detrás de CL-STA-1132 en herramientas de código abierto, en lugar de malware propietario, redujo la detección basada en firmas y facilitó una integración discreta dentro de los entornos comprometidos. Esta elección técnica, junto con una cadencia operativa disciplinada de sesiones interactivas intermitentes durante varias semanas, permitió mantenerse deliberadamente por debajo de los umbrales de detección de la mayoría de los sistemas automatizados de alerta", agregó la compañía.